AF/RK

NEIFELD IP LAW, P.C.
4813-B Eisenhower Avenue
Alexandria, Virginia 22304

Tel: 703-415-0012

Fax: 703-415-0013
Email: rneifeld@Neifeld.com
Web: www.Neifeld.com

TRANSMITTAL LETTER AND AUTHORIZATION TO CHARGE DEPOSIT ACCOUNT

ASSISTANT COMMISSIONER FOR PATENTS
ALEXANDRIA, VA 22313

RE: Attorney Docket No.: SIEM0023U-USCP
Application Serial No.: 09/513,462
Confirmation No.: 7313
Filed: 02/25/00
Title: Method for Using Software Products that are Offered Via a Network
Inventor: Markus LAUTENBACHER
Group Art Unit: 3622
Examiner: BACKER, F.

SIR:

Attached hereto for filing are the following papers:
CHECK for $500.00
37 CFR 41.37 APPEAL BRIEF (52 PAGES)

Our check in the amount of $500.00 is attached covering the required fees.

The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 50-2106. A duplicate copy of this sheet is enclosed.

31518
PATENT TRADEMARK OFFICE

4/11/2005
Date

Robert G. Crockett
Registration No. 42,448

Printed: April 11, 2005 (3:21pm)
Y:\Clients\Siemens\SIEM0023UUSCP\Drafts\Transmittal Letter_040624.wpd

DOCKET NO: SIEM0023U-USCP

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: CONFIRMATION NO.:7313

Markus LAUTENBACHER GROUP: 3621

APPLICATION NUMBER: 09/513,462 EXAMINER: BACKER, F.

FILED: February 25, 2000

FOR: Method for Using Software Products that are Offered Via a Network

BOX STOP APPEAL BRIEF - PATENTS
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

37 CFR 41.37 APPEAL BRIEF

Sir:

In reply to the non-final Office action mailed October 12, 2004, applicant appeals the rejection to the Board of Patent Appeals and Interferences because the claims of this application for patent have been twice-rejected.

04/12/2005 MBIZUNES 00000068 09513462
01 FC:1402 500.00 OP

Table of Contents

I. **37 CFR 41.37(c)(1)(i) Real Party in Interest**

The real party in interest is SIEMENS Aktiengesellschaft, a German corporation.

II. **37 CFR 41.37(c)(1)(ii) Related Appeals and Interferences**

There are no related pending appeals, pending interferences, or requests for interferences known to the appellant's representative or the appellant's assignee.

III. **37 CFR 41.37(c)(1)(iii) Status of Claims**

Claims 1 and 3-15 are pending, rejected, and under appeal.

IV. **37 CFR 41.37(c)(1)(iv) Status of Amendments**

All amendments are entered.

V. **37 CFR 41.37(c)(1)(v) Summary of the Claimed Subject Matter**

The invention of claim 1 is a method for using software products that are offered via a network, comprising: inquiring about a software product from an offer server by a user via a terminal device (page 7 lines 11-15); downloading said software product from said offer server via said network onto said terminal device in response to said inquiring by said user (page 7 lines 14-15; page 12 lines 16-23); activating a software component of said software product (page 7 lines 16-19; page 12 line 28 to page 13 line 7); starting a communication by way of said software component with a usage processing server regarding a usage of said software product in response to a call of said software product in said terminal device of said user, wherein said usage processing server is operated by a network provider (page 7 lines 16-19; page 13 lines 8-9); providing, by said software component in a framework of said communication, data to said usage processing server; (page 7 lines 23-26; page 9 lines 5-15) and checking said data, by said usage processing server (page 7 line 27 to page 8 line 8; page 13 lines 9-12), and then making a determination selected from a group consisting of: whether usage of said software product is approved with respect to said inquiring user (page 8 lines 9-14), and whether charging operations are carried out on user accounts and provider of software product accounts (page 8 lines 15-22; page 13 lines 13-15; page 12 line 17 to page 14 line 9).

The invention of claim 5 is a usage processing server comprising: a usage processing module for processing a software product downloaded from a network (page 7 lines 4-10); wherein said usage processing server is operated by a network provider (page 7 lines 16-19; page

13 lines 8-9) and wherein said usage processing server is contacted by said software product after said software product has been downloaded into a terminal device of a user and has been activated (page 7 lines 16-19; page 12 line 28 to page 13 line 7); and wherein usage processing data required to perform usage processing are delivered to said usage processing server (page 7 lines 23-26; page 9 lines 5-15).

The invention of claim 11 is a software product, comprising: a software component that is activated when called by said software product (page 7 lines 16-19; page 12 line 28 to page 13 line 7) and that subsequently starts communicating with a usage process server and delivers usage processing data required for performing usage processing to said usage processing server in the framework of said communication, wherein said usage processing server is operated by a network provider (page 7 lines 23-26; page 9 lines 5-15); wherein said software product can be downloaded into a terminal device by a user via a network in response to an inquiry from said user (page 7 lines 11-15).

The invention of claim 14 is a method for the generation of a software product that is offered via a network, comprising: installing a software component in source code of said software product of a software manufacturer by using a software development kit provided by a usage processing provider (page 7 lines 14-15; page 12 lines 16-23); activating said software component when called by said software product (page 7 lines 16-19; page 12 line 28 to page 13 line 7); starting a communication by said software component with a usage processing server after said activating said software component, wherein said usage processing server is operated by a network provider (page 7 lines 16-19; page 13 lines 8-9); sending, by said software component, usage processing data that are required for performing usage processing to said usage processing server in the framework of said communication (page 7 lines 23-26; page 9 lines 5-15).

The invention of claim 15 is a method for using software products that are offered via a network, comprising: inquiring about a software product from an offer server by a user via a terminal device (page 7 lines 11-15); downloading said software product from said offer server via said network onto said terminal device in response to said inquiring by said user (page 7 lines 14-15; page 12 lines 16-23); activating a software component of said software product (page 7

lines 16-19; page 12 line 28 to page 13 line 7); starting a communication by way of said software component with a usage processing server regarding a usage of said software product in response to a call of said software product in said terminal device of said user (page 7 lines 16-19; page 13 lines 8-9); providing, by said software component in a framework of said communication, data to said usage processing server; (page 7 lines 23-26; page 9 lines 5-15) and checking said data, by said usage processing server (page 7 line 27 to page 8 line 8; page 13 lines 9-12), and then making a determination selected from a group consisting of: whether usage of said software product is approved with respect to said inquiring user (page 8 lines 9-14), and whether charging operations are carried out on user accounts and provider of software product accounts (page 8 lines 15-22; page 13 lines 13-15; page 12 line 17 to page 14 line 9).

VI. **37 CFR 41.37(c)(1)(vi) Grounds for Rejection To Be Reviewed On Appeal**

Whether the rejection of claim 11 under 35 USC 101 as being directed to non-statutory subject matter should be reversed.

Whether the rejection of claims 5-14 under 35 USC 102(e) as being anticipated by Krishnan et al. (U.S. PG Pub no. 2001/0011254) ("Krishnan") should be reversed.

Whether the rejection of claims 1, 3, 4, and 15 under 35 USC 103(a) as being unpatentable over Krishnan in view of U.S. patent 5,925,127 to Ahmad et al. ("Ahmad") should be reversed.

VII. **37 CFR 41.37(c)(1)(vii) Argument**

A. **The Rejection Under 35 USC 101 of Claim 11**

1. **The Examiner's Argument**

In support of the rejection of claim 1 under 35 USC 101 as being directed to non-statutory subject matter, the examiner states that:

> 3. Claim 11 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.
>
> The basis of this rejection is set forth in a two prong test of:
>
> (1) whether the invention is within the technological arts; and
>
> (2) whether the invention produces a useful, concrete and tangible result.

For a claimed to be statutory, the claimed invention must be within the technological arts.

Mere ideas in the abstract (i.e., abstract idea law of nature, natural phenomena) that do not apply,

involve, use, or advance the technological arts fail to promote the "progress of science and the useful arts" and therefore are found to be non-statutory subject matter. For a method claim to pass the muster, the recited method must somehow apply, involve, use, or advance the technological arts

In the present case the inventive concept in claim 11 is directed to software product. It, However, fails to clearly disclose what type of software product being claimed and fail to produce a useful concrete and tangible result. Therefore deemed to be directed to non-statutory subject matter. [Office action mailed 3/24/2004 at page 2 item 3.]

2. **The Recitation of Claim 11**

11. A software product, comprising:

a software component that is activated when called by said software product and that subsequently starts communicating with *a usage process server* and delivers usage processing data required for performing usage processing to said usage processing server in the framework of said communication, wherein said usage processing server is operated by a network provider;

wherein said *software product can be downloaded into a terminal device by a user via a network* in response to an inquiry from said user. [Emphasis added.]

3. **Claim 11 Recites Subject Matter Within the Technological Arts**

Claim 11 recites "...a usage process server...wherein said software product can be downloaded into a terminal device by a user via a network ...." The applicant respectfully submits that because claim 11 recites "...a usage process server...wherein said software product

can be downloaded into a terminal device by a user via a network ..,"the subject matter of claim 11 is within the technological arts and satisfies the requirements of 37 CFR 101. A "usage process server,"a "terminal device" and "a network," recited in claim 11, are clearly concrete, technological components that are not "ideas in the abstract." Claim 11, therefore, defines a concrete, tangible apparatus that implements the claimed method to achieve a useful, concrete, and tangible result. Therefore, claim 11 is directed to statutory subject matter and satisfies the requirements of 37 CFR 101. Therefore, the applicant respectfully submits that the rejection of claim 11 under 35 USC 101 is improper and should be reversed.

B. **The Rejection of Claim 5 Under 35 USC 102(e) as Being Anticipated by Krishnan et al (U.S. Patent No. 6,073,124) ("Krishnan")**

1. **The Examiner's Argument**

As per claim 5, Krishman et al teaches usage processing server comprising a usage processing module for processing a software product download from a network, and wherein usage processing data required to perform usage processing are delivered to the usage processing server wherein the usage processing server is contacted by the software product after the software product has been downloaded into a terminal device of a user and has been activated, and wherein the usage processing data required to perform usage processing are delivered to the processing server (*see figs 2, 3, summary of the invention and column 6 lines 44-7 lines 43, 8 lines 33-12 line 59*). [Office Action mailed October 12, 2004 page 3 line 25 through page 4 line 8.]

2. **The Citations From Krishnan Relied Upon By the Examiner**

In rejecting claim 5, the examiner relies upon the the Summary of the Invention of Krishnan at column 4 line 10 to column 5 line 32, which states that:

The present invention provides methods and systems for facilitating the purchase and delivery of electronic content using a secure digital commerce system. The secure digital commerce system interacts with an online purchasing

system to purchase and distribute merchandise over a network. The secure digital commerce system is comprised of a plurality of modularized components, which communicate with each other to download, license, and potentially purchase a requested item of merchandise. Each component is customizable.

Exemplary embodiments of the secure digital commerce system ("DCS") include a DCS client and a DCS server. The DCS client includes a plurality of client components, which are downloaded by a boot program onto a customer computer system in response to requesting an item of merchandise to be licensed or purchased. The downloaded client components include a secured (e.g., encrypted) content file that corresponds to the content of the requested item and licensing code that is automatically executed to ensure that the item of merchandise is properly licensed before a customer is permitted to operate it. The DCS server includes a content supplier server, which provides the DCS client components that are specific to the requested item, and a licensing and purchasing broker, which generates and returns a secure electronic licensing certificate in response to a request to license the requested item of merchandise. The generated electronic license certificate contains licensing parameters that dictate whether the merchandise is permitted to be executed. Thus, once properly licensed, the downloaded client components in conjunction with the electronic license certificate permit a legitimate customer to execute (process) purchased content in a manner that helps prevent illegitimate piracy.

In one embodiment, the electronic license certificate is generated from tables stored in a password generation data repository. Each table contains fields that are used to generate the license parameters. Each electronic license certificate is generated specifically for a particular item of merchandise and for a specific customer request. Also, the electronic license certificate is secured, such as by encryption, to prevent a user from accessing the corresponding item of merchandise without proper authorization. One technique for securing the electronic license certificate uses a symmetric cryptographic algorithm.

The secure digital commerce system also supports the ability to generate emergency electronic license certificates in cases where an electronic license certificate would not normally be authorized. To accomplish this objective, a separate emergency password generation table is provided by the password generation data repository. In addition, the secure digital commerce system reliably downloads the client components even when a failure is encountered during the download procedure. Further, a minimum number of components are downloaded.

In addition to generating electronic license certificates, the licensing and purchasing broker may also include access to a payment processing function, which is invoked to authorize a particular method of payment for a particular transaction. The licensing and purchasing broker may also include access to a clearinghouse function used to track and audit purchases.

Digital commerce is performed using the secure digital commerce system as follows. A customer invokes an online purchasing system to request an item of merchandise and to indicate a purchasing option (such as "try" or "buy"). The DCS client then downloads onto a customer computer system the client components that are associated with the requested item. Included in these components is a secured content component. The secured content component is then installed and executed (processed) in a manner that automatically invokes licensing code. The licensing code, when the requested item is not yet licensed properly, causes the requested item to be licensed by the licensing and purchasing broker in accordance with the indicated purchasing option before the content component becomes operable. Specifically, the licensing and purchasing broker generates a secure electronic license certificate and completes an actual purchase when appropriate. The broker then returns the electronic license certificate to the licensing code, which unsecures (e.g., unencrypts) and deconstructs the electronic license certificate to determine the licensing parameters. The licensing code then executes (processes) the content component in accordance with the license

parameters.

In some embodiments, the secure digital commerce system supports the licensing and purchasing of both merchandise that is deliverable online and merchandise that requires physical shipment of a product or service (e.g., non-ESD merchandise). [Krishnan at column 4 line 10 to column 5 line 32.]

In rejecting claim 5, the examiner further relies upon the following passage from Krishnan at column 6 line 44 to column 7 line 43, which states that:

FIG. 2 is an example display screen of an online virtual store that operates with the secure digital commerce system. Although the secure digital commerce system is described with reference to a virtual store, one skilled in the art will recognize that any type of electronic purchasing system or application, including a standalone application, is operable with embodiments of the present invention. A browser application window 201 is shown currently displaying (and executing) a WEB page 202 retrieved from the location specified by the URI "www.buysoftware.com." WEB page 202 provides a set of user interface elements, for example, pushbuttons 204 and 205 and icon 203 which display information or which can be used to navigate to additional information. A virtual store typically provides a set of icons, which each describe an item of merchandise that can be purchased. For example, graphical icon 203 is an example icon that is linked to the functionality needed to purchase a Microsoft Corp. software game entitled "RETURN OF ARCADE."

Each icon is typically linked to a server site on the network, which is responsible for supplying the content of the item when purchased if the item is capable of electronic delivery. When the user selects one of the icons, the browser application, as a result of processing the link, sends a request for the selected item to the server site. Thus, when a customer selects the icon 203, an HTTP request message is sent to an appropriate server site to locate and download the software modules that correspond to "RETURN OF ARCADE."

For the purposes of this specification, the merchandise that can be licensed and distributed online includes any type of digital or electronic, information or data that can be transmitted using any means for communicating and delivering such data over a network, including data transmitted by electronics, sound, laser, or other similar technique. Similarly, although the present application refers generically to "electronic data" or "electronic content," it will be understood that embodiments of the present invention can be utilized with any type of data that can be stored and transmitted over a network.

The secure digital commerce system is arranged according to a client/server architecture and provides a modularized DCS client and a modularized DCS server that interact with the online purchasing system to perform a purchase. The DCS client includes a set of client components; support for downloading the client components onto a customer computer system; and support for communicating with the DCS server to license an item of merchandise. The client components contain a secured (e.g., encrypted) copy of the content and various components needed to license and purchase the merchandise and to unsecure (e.g., decrypt) and execute the licensed merchandise. The DCS client communicates with the DCS server to download the client components onto a customer's computer system in response to a request for merchandise from the online purchasing system. The DCS client also communicates with the DCS server to license and purchase the requested merchandise. The DCS server generates an electronic license certificate, which contains license parameters (e.g., terms) that are specific to the requested merchandise and to a desired purchasing option (such as trial use, permanent purchase, or rental). The DCS server then sends the generated electronic license certificate to the DCS client. Once a valid electronic license certificate for the requested merchandise is received by the DCS client, the merchandise is made available to the customer for use in accordance with the license parameters contained in the electronic license certificate. [Krishnan at column 6 line 44 to

column 7 line 43.]

In rejecting claim 5, the examiner further relies upon the following extensive passage from Krishnan at column 8 line 33 to column 12 line 59, which states that:

> FIG. 3 is an overview block diagram of the secure digital commerce system. FIG. 3 includes a DCS client 301 and a DCS server 302, which are used with an online purchasing application, such as a WEB browser application 303, to provide a purchasing interface for a potential customer. The DCS client 301 includes a virtual store 304 and a data repository 305. The virtual store 304 provides a customer front end 312 and stores in the data repository 305 merchandise-specific download files 313. The customer front end 312 includes WEB pages and associated processing support, which are downloaded onto a customer computer system 311 to enable a user to purchase merchandise. The download files 313, which each contain an executable boot program and a component list, are used to download the merchandise-specific client components (for example, a secured content file and licensing code). When an item of merchandise is requested, the associated download file is processed to extract the executable boot program and the component list. The executable boot program downloads the needed components from the content supplier server 306 using the component list, which specifies the components that are needed to successfully license and operate the corresponding item of merchandise. In an alternate embodiment, download files are generated dynamically from component lists, which lists are stored in the data repository 305.
>
> The DCS server 302 includes a content supplier server 306, a licensing and purchasing broker (server) 307, a password generation data repository 308, and a payment processing function 309. The licensing and purchasing broker 307 includes a separate licensing library 310 (passgen.dll), which contains the code for generating an appropriate license in response to a request from the virtual store. The licensing library 310 uses the password generation data repository 308 to

generate an electronic license certificate ("ELC") with licensing parameters that correspond to a particular item of merchandise. An electronic license certificate is encrypted electronic data that provides information that can be utilized to determine whether a particular customer is authorized to execute the merchandise. Such information may include, for example, the specification of a period of time that a particular customer is allowed to execute the merchandise for trial use. The data repository 308 contains tables and fields that are used to create the license parameters of a license. The data repository 308 may contain information that is supplied by the source companies of the available merchandise. The payment processing functions 309 are used by the licensing and purchasing broker 307 to charge the customer and to properly credit the appropriate supplier when the customer requests an actual purchase (rather than trial use or another form of licensing). In addition, clearinghouse functions may be invoked by the licensing and purchasing broker 307 to audit and track an online purchase. Clearinghouse functions may be as provided by well-known commercial sources, such as Litlenet and Cybersource. Similarly, payment processing functions may be provided using well-known commercial credit card authorization services.

FIG. 4 is an overview flowchart of the example steps performed by the secure digital commerce system components to perform the licensing and purchase of electronic data. This figure briefly describes the interactions between the components shown in FIG. 3 to accomplish the downloading, licensing, and purchasing of a requested item of merchandise when it can be delivered online. In step 401, the potential customer downloads a WEB page (part of the customer front end 312) from the virtual store 304 that includes the item to be requested (see, for example, FIG. 2). In step 402, the customer requests an item of merchandise, for example, by selecting an icon that is linked to a download file that corresponds to the desired item. In response to the selection, in step 403, the virtual store 304 downloads and installs the download file, which extracts the executable boot program and component list and causes execution (preferably as a

background task) of the executable boot program on the customer computer system 311. In step 404, the boot program reads the component list to determine what DCS client components to download and requests the determined components from the appropriate contents supplier server 306. The component list, as further described below with reference to Table 2, indicates source and target locations for each component to be downloaded. In step 405, the boot program installs a downloaded (secured) content file that is associated with the desired item of merchandise and causes the content file to be processed (executed). When the content file is a computer program, then the downloaded content file has been previously configured to automatically cause licensing code to be executed before the content file is executed. When instead the content file is data to be input to a computer program, then the content player is previously configured to automatically cause the licensing code to be executed first before the content file data is processed. More specifically, the downloaded content player is installed by the boot program to process the secured (e.g., encrypted) content file data. The boot program then starts the execution of the content player, which invokes and causes execution of the downloaded licensing code. Thus, in step 406, the licensing code, which is incorporated into either the content file or the content player, is executed. In step 407, if the licensing code determines that a valid ELC already exists, then the content file continues to be processed in step 412, else the licensing code continues in step 408. In step 408, the licensing code requests a valid ELC from the licensing and purchasing broker 307. In step 409, the licensing and purchasing broker 307 determines whether a purchase is requested and, if so, continues in step 410, else continues in step 411. In step 410, the licensing and purchasing broker 307 obtains a method for payment and authorizes the payment method using the payment processing function 309. In step 411, the licensing and purchasing broker 307 generates an appropriate ELC using the licensing library 310 and the password generation data repository 308 and returns the generated EL-C to the licensing code. In step 412, if portions of

the content file are encrypted as will be further described, then the content file is decrypted and processed.

As indicated above, when the downloaded (secured) content file is a computer program, licensing code is automatically invoked to verify the existence of, or obtain, a valid electronic license certificate for a requested item and to decrypt and execute the content file. One mechanism for incorporating licensing code into a content file such that it is automatically invoked is discussed in detail with reference to related U.S. patent application Ser. No. 08/792,719, entitled "Method and System for Injecting New Code Into Existing Application Code," filed on Jan. 29, 1997. That patent application describes a technique for inserting licensing code into an existing application and for inserted security code that securely executes the application code. The security code uses an incremental decryption process to ensure that a complete version of the unmodified application code is never visible at any one time (to avoid illegitimate copying). Thus the security code mechanism described therein makes it impossible for someone to create an unmodified version of the application in a reasonable amount of time. The insertion technique described therein can be used to insert into a content file the licensing code component of the DCS client, which communicates with the licensing and purchasing broker to generate an ELC. Further, the encryption/decryption technique described therein may be used in the current context to incorporate security code that securely decrypts and executes the downloaded content file.

In addition, when the content file is data to be used as input to a computer program (such as a content player), then the licensing code can be incorporated into the computer program by invoking licensing code and security code routines. For example, an application programming interface ("API") to the licensing code and to the incremental decryption security code can be provided. The content player is programmed (or configured via the insertion technique described in the related patent application) to include calls to the API routines to validate or obtain

an ELC and to unsecure (e.g., decrypt) the associated content file. One skilled in the art will recognize that any mechanism that automatically causes the execution of licensing code (and security code) before the secured content is processed is operable with embodiments of the present invention.

In exemplary embodiments, the DCS client is implemented on a computer system comprising a central processing unit, a display, a memory, and other input/output devices. Exemplary embodiments of the DCS client are designed to operate in a globally networked environment, such as a computer system that is connected to the Internet. FIG. 5 is a block diagram of a general purpose computer system for practicing embodiments of the DCS client. The computer system 501 contains a central processing unit (CPU) 502, a display 503, a computer memory (memory) 505, or other computer-readable memory medium, and other input/output devices 504. Downloaded components of the DCS client preferably reside in the memory 505 and execute on the CPU 502. The components of the DCS client are shown after they have been downloaded and installed on the computer system 501 by an executable boot program and after an appropriate electronic license certificate has been generated and installed. Specifically, the components of the DCS client include the executable boot program 507 (SAFEboot); a user interface library 508 (SAFEUI.dll); a purchasing request library 509 (SAFEBuy.dll); an encrypted content file 510, which is shown with incorporated licensing code 511 (SAFE.dll); an encrypted DCS security information file 512, which is associated with the encrypted content file 510; and an electronic licensing certificate 514 (ELC). As shown, each library is typically implemented as a dynamic link library (a "DLL"). In addition to these components, when the encrypted content file contains data that is not a computer program, the memory 505 contains a content player 513 for processing the content file 510, which has incorporated licensing code 511. Also, WEB browser application code 506 is shown residing in the memory 505. Other programs 515 also reside in the memory 505. One skilled in the art will recognize that

exemplary DCS client components can also be implemented in a distributed environment where the various programs shown as currently residing in the memory 505 are instead distributed among several computer systems. For example, the encrypted content file 510 may reside on a different computer system than the boot program 507.

In exemplary embodiments, the DCS server is implemented on one or more computer systems, each comprising a central processing unit, a memory and other input/output devices. Each of these computer systems may be a general purpose computer system, similar to that described in FIG. 5, which is connected to a network. The server systems that comprise the server portion may or may not include displays. The password generation data repository may be implemented using any well-known technique for implementing a database or any other type of data repository. Although shown as a separate facility, one skilled in the art will recognize that the data repository may be incorporated as a component of the computer system that is used to implement the licensing and purchasing broker. Further, one skilled in the art will also recognize that a variety of architectures are possible and can be used to implement exemplary embodiments of the DCS server.

FIG. 6 is an example flow diagram of the steps performed to generate the components of the DCS client. In an exemplary embodiment, these steps are performed by a utility program referred to as the SAFEmaker utility. The SAFEmaker utility is responsible for generating the downloadable components that correspond to an item to be supplied as online merchandise. In addition, the utility generates a secured content file that can only be processed when access is granted. This capability is referred to as making the file "SAFE" (hence, the SAFE-prefix in the component names). Making a content file "SAFE" implies that security code and licensing code are incorporated into the content file (or content player, in the case of digital content that is not a computer program) to ensure that the online merchandise is usable only when proper licensing has been performed.

Typically, this process involves encrypting some portion of the content file. Some components generated by the SAFEmaker utility are stored on the content supplier server (e.g., content supplier server 306 in FIG. 3) and are downloaded in response to requests from the virtual store front end. Other components are stored on the virtual store, which may be located on a different computer system from the content supplier server. The SAFEmaker utility also updates the password generation data repository of the DCS server with merchandise-specific information.

Specifically, in step 601, the utility incorporates licensing and security code into the supplier specific electronic content or content player. As described above, an exemplary embodiment incorporates licensing and security code according to the techniques described in the related U.S. patent application Ser. No. 08/792,719, entitled "Method and System for Injecting New Code into Existing Application Code," filed on Jan. 29, 1997 or by calling routines of an API as appropriate (e.g., when a content player is needed). One skilled in the art, however, will recognize that any technique for ensuring that proper licensing code gets executed when the content is processed and for encrypting (and subsequently decrypting) the content file will operate with embodiments of the present invention. In step 602, the utility produces one or more files that contain the (partially or fully) encrypted content. In step 603, the utility produces an encrypted DCS security information file(s), which contain information that is used, for example, to decrypt the content and to produce a proper license. The contents of an encrypted DCS security information file are described in further detail below with reference to Table 1. In step 604, the utility creates a component list file (an ".ssc" file) and a download file for this particular online merchandise. Specifically, in an embodiment that statically generates download files, a self-extracting installation file is generated (the download file), which contains the component list file (an ".ssc" file) specific to the merchandise and the executable boot program. As described above, the download file, which contains the

executable boot program and the component list, is typically stored on the virtual store computer system. The executable boot program uses the component list file to determine the components to download and to download them when particular electronic content is requested. An example component list file is described further below with reference to Table 2. In step 605, the utility stores the download file on the virtual store computer system (e.g., virtual store 304 in FIG. 3). When instead the download files are dynamically generated by the virtual store when needed for a particular WEB page, then in steps 604 and 605, the utility creates and stores only the component list file. In step 606, the utility stores the other components of the DCS client, for example, the encrypted content and DCS security information files, the licensing code, and the user interface library on the content supplier server system (e.g., content supplier server 306 in FIG. 3). In step 607, the utility updates the password generation data repository (e.g., password generation database 308 in FIG. 3) with the merchandise-specific licensing information, for example, the fields used to generate the license parameters of a valid electronic license certificate, and then returns. An example password generation data repository is discussed in further detail with reference to Tables 3, 4, and 5. One skilled in the art will recognize that the generation of these components and the password generation data may be performed at different times and by separate utilities. [Krishnan at column 8 line 33 to column 12 line 59]

3. The Applicant's Argument - Claim 5

a. The Recitation of Claim 5

5. A usage processing server comprising:

a usage processing module for processing a software product downloaded from a network;

wherein said *usage processing server is operated by a network provider* and wherein said usage processing server is contacted by said software product after said software product has been downloaded into a terminal device of a user

and has been activated; and

wherein usage processing *data required to perform usage processing* are delivered to said usage processing server. [Emphasis added.]

b. **The Applicant's Disclosure Supporting Claim 5**

i. **The Applicant's Definition of "Network Provider"**

The application's definition of "network provider" is clear from the following passage in the specification of this application:

> The network operator (or "*network provider*") operates and administers a network that primarily provides a "bit-transport" functionality . The network operator provides network connectivity for the web servers of the provider of software and contents or he may assume this function vicariously by providing a web server for the provider ("web hosting") . The network operator also *provides network connectivity for the end user*, normally as dial-in via a modem or ISDN, and thus normally has an *established and long term business relationship with the end user*: He sends the end user invoices about received network connectivity performances on a regular basis and knows his financial actions. [Specification at page 1 lines 15-23; emphasis added.]

ii. **The Applicant's Definition of "Usage Processing"**

The application's definition of "usage processing" is clear from the following passage in the specification of this application:

> According to the present invention, a service provider (e.g., the network operator) assumes the *usage processing*, (e.g., "*charging and/or access control*") for the usage of software and contents. The network operator offers this as a service for the provider of software and contents, when the provider wishes to "outsource" these tasks in order to be able to concentrate on the preparation of software and contents.The provider of software and contents can also avoid the *charging of very small amounts*, which may not be economical for him, via

"outsourcing".

Providing *usage processing*, such as *charging and/or access control*, is particularly advantageous for the network operator since the end user is already connected to the network of the network operator for purposes of the network connectivity, and therefore is in a *long term business relationship* with the network operator. [Specification at page 4 lines 1-13; emphasis added.]

The application's definition of "usage processing" is clear from the following passage in the specification of this application:

Step 3 : When someone *calls the software* and contents, the service module, which is introduced via the software development kit for purposes of controlling the access and charging, *contacts the corresponding server* of the network operator via the network; *this takes place immediately after the start of the software and contents* . This contact between the service module and server via the network requires an always-on network connection or at least requires a sufficiently fast dial-up-on-demand method at the end user side . For purposes of controlling the access and charging, *data, such as cryptographic identification character (a one-to-one corresponding identification number or valid charging model) of the software and contents, user data (a user identification character, password, or account number)*, are thereby transferred to the network operator.

Step 4 : The network operator checks the data received by the end user regarding correctness, topicality and compatibility of the profile that is preset by the customer . When the end user inquires about the usage of specific software and contents, the following exemplary information can be co-considered on the server of the network operator : the cryptographic identification character and version number of the software and contents, the type of the software and contents to be used with respect to a *preset user profile (such as age restriction, restriction with respect to specific contents, etc .) of the end user, and the creditworthiness and account balance of the end user* . Such a finely-adjusted checking could not

be performed in a secure manner on the device of the end user.

At the end of the check, the server of the network operator, via the network connection, reports back to the corresponding access control- and charging model on the side of the end user whether the end user is allowed to use the software and contents : If so, the software and contents continues with its *normal functioning* ; if not, the access control- and charging model terminates the software and contents with an error message and thus prevents their unauthorized usage by the end user . [Specification at page 7 line 16 to page 8 line 14; emphasis added.]

c. **Disputed Factual Assertion - Krishnan Does Not Teach or Suggest "...a usage processing server...operated by a network provider..." As Recited in Claim 5**

The applicant respectfully submits that the citations to Krishnan relied upon by the examiner in rejecting claim 5 do not teach or suggest "...a usage processing server...operated by a network provider," as recited in claim 5.

i. **Krishnan's "DCS Server" Is Not a "Network Provider" As Recited in Claim 5**

Krishnan's DCS server 302 is not "...a network provider..." as recited in claim 5. Krishnan discloses at column 8 line 59 to column 9 line 2 that the functions of his DCS server 302 are:

The DCS server 302 includes a content supplier server 306, a licensing and purchasing broker (server) 307, a password generation data repository 308, and a payment processing function 309. The licensing and purchasing broker 307 includes a separate licensing library 310 (passgen.dll), which contains the code for generating an appropriate license in response to a request from the virtual store. The licensing library 310 uses the password generation data repository 308 to generate an electronic license certificate ("ELC") with licensing parameters that correspond to a particular item of merchandise. [Krishnan at column 8 line 59 to column 9 line 2.]

Krishnan does not disclose that his DCS Server 302 is a network provider providing *internet access to end users.* The Krishnan system is only capable of electronic commerce over a pre-existing network in which connectivity has previously been provided and maintained between end users and "online purchasing systems." Nothing in Krishnan's disclosure indicates that Krishnan's DCS Server 302 interacts directly with end users in the manner that a network provider, as disclosed in this application, interacts with end users. Therefore, one of ordinary skill in the art would recognize that Krishnan's "DCS Server 302" is not a "network provider" as recited in claim 5.

ii. **Conclusion: Claim 5 Is Not Anticipated By Krishnan**

Claim 5 recites "a usage processing server...operated by a network provider." For the reasons given above, Krishnan does not disclose or suggest "a usage processing server...operated by a network provider." Therefore, Krishnan does not teach or suggest the subject matter of claim 5. Therefore, Krishnan does not anticipate claim 5. Therefore, the rejection of claim 5 under 35 USC 102(e) is improper and should be reversed.

d. **Disputed Factual Assertion - Krishnan's System Does Not Disclose or Suggest "...usage processing data required to perform usage processing..." As Recited in Claim 5**

Krishnan's system is directed to the purchase and delivery of electronic content, in contrast to "usage processing," as recited in claim 5 and disclosed in the specification of this application. The claimed "usage processing" comprises, for example, processing accounting information and user profiles *each and every time a program is used.* Krishnan's system is limited to delivering an electronic license to a client system. Once the electronic license is present on the client system, the target software can be used an unlimited number of times by any user of the client system. Krishnan does not disclose or suggest the "usage processing" of accounting information, for example, related to the user's use of a particular program *each and every time that particular program is used.*

i. **Krishnan's System Discloses the Purchase and Delivery of Electronic Content; It Does Not Disclose or Suggest "...usage processing data..." As Recited in Claim 5**

In contrast to the applicant's system, the "download file 313" and the "boot program" taught by Krishnan are limited to downloading components onto a client system, as disclosed by Krishnan at column 8 lines 33-58 that:

> FIG. 3 is an overview block diagram of the secure digital commerce system. FIG. 3 includes a DCS client 301 and a DCS server 302, which are used with an online purchasing application, such as a WEB browser application 303, to provide a purchasing interface for a potential customer. The DCS client 301 includes a virtual store 304 and a data repository 305. The virtual store 304 provides a customer front end 312 and stores in the data repository 305 merchandise-specific download files 313. The customer front end 312 includes WEB pages and associated processing support, which are downloaded onto a customer computer system 311 to enable a user to purchase merchandise. The *download files 313, which each contain an executable boot program and a component list, are used to download the merchandise-specific client components* (for example, a secured content file and licensing code). When an item of merchandise is requested, the associated download file is processed to extract the *executable boot program* and the component list. The *executable boot program* downloads the needed components from the content supplier server 306 using the component list, which specifies the components that are needed to successfully license and operate the corresponding item of merchandise. In an alternate embodiment, download files are generated dynamically from component lists, which lists are stored in the data repository 305. [Krishnan at column 8 lines 33-58; emphasis added.]

Clearly, one of ordinary skill in the art would recognize that Krishnan's "boot program," as disclosed, is not designed to transmit "usage data" each time the target software is executed, as

defined by claim 5. The data transmitted by the Krishnan system is only a list of "needed components." Krishnan's "electronic license certificate ("ELC")" cannot function as the claimed "usage data" because Krishnan's does not contain data useful to determining, for example, the identity or financial status of the user, such as a user identification character, password, or account number. The Krishnan's "electronic license certificate ("ELC")" can *only* function to control the purchase of software and cannot be used for the purpose, for example, of charging the end user for *each use* of software. This is because once the end user has possession of "electronic license certificate ("ELC")," Krishnan's DCS Server 302 will allow the end user to execute the software as many times as the end user wishes. Therefore Krishnan does not disclose or suggest "usage data," as recited by claim 5. Likewise, Krishnan does not teach or suggest "...a usage processing server..," as recited by claim 5.

ii. **Conclusion: Claim 5 Is Not Anticipated By Krishnan**

Claim 5 recites "usage processing data required to perform usage processing." For the reasons given above, Krishnan does not disclose or suggest "usage processing data required to perform usage processing." Therefore, Krishnan does not teach or suggest the subject matter of claim 5 because Krishnan does not disclose each and every limitation of claim 5. Therefore, Krishnan does not anticipate claim 5. Therefore, the rejection of claim 5 under 35 USC 102(e) is improper and should be reversed.

e. **Krishnan's System Requires That an Electronic License Certificate ("ELC") Be Installed On User's Computer; This Compomises Security**

Krishnan states at column 8 line 59 to column 9 line 9 that:

> The DCS server 302 includes a content supplier server 306, a licensing and purchasing broker (server) 307, a password generation data repository 308, and a payment processing function 309. The licensing and purchasing broker 307 includes a separate licensing library 310 (passgen.dll), which contains the code for generating an appropriate license in response to a request from the virtual store. The licensing library 310 uses the password generation data repository 308 to generate an electronic license certificate ("ELC") with licensing parameters that

correspond to a particular item of merchandise. An electronic license certificate is encrypted electronic data that provides information that can be utilized to determine whether a particular customer is authorized to execute the merchandise. Such information may include, for example, the specification of a period of time that a particular customer is allowed to execute the merchandise for trial use. [Krishnan at column 8 line 59 to column 9 line 9.]

In contrast to the invention defined by claim 5, Krishnan requires that an Electronic License Certificate ("ELC") be installed on DCS Client 301. In Krishnan's system, the Electronic License Certificate is created by licensing and purchasing broker 307. Because the Electronic License Certificate is created by licensing and purchasing broker 307, the Electronic License Certificate cannot contain "usage data," such as, for example, a "cryptographic identification character (a one-to-one corresponding identification number or valid charging model) of the software and contents, user data (a user identification character, password, or account number," which may be used to control access to complete software programs and to charge the user for use of software. Further, because the user has explicit possession of the key, Krishnan's Electronic License Certificate can be passed to another party or can be stolen, creating a security breach, thereby rendering Krishnan's system ineffective for "usage processing" as recited in claim 5.

The "usage data" recited in claim 5 is completely different from Krishnan's "Electronic License Certificate ("ELC")." Support for "usage data," as recited in claim 5, can be found for example, in the specification of this application at 9 lines 5-30, which states:

> The CIDAA request generator of the CIDAA module places a request via the network of the network operator for purposes of controlling the access and charging with respect to the CIDAA request handler on the corresponding server of the network operator. A cryptographic identification character that is specific for the respective software and content is thereby transferred in the direction of the network operator in the form of a what is referred to as MD5 digest, as well as an *identification character and password of the end user.* Prior to this, the CIDAA

module requests the end user to input the identification character and password. *MD5 is a special type of the general class of "hash functions"*, which are used in order to *biuniquely reduce digital signatures of digital data to "message digests"* for purposes of improved handling.

The "CIDAA decision maker" takes different criteria into consideration in order to decide whether to allow the inquiry of the end user to use the software and contents.

Possible criteria are:

a) the correct cryptographic identification character of the software and contents, registered at the network operator ;

b) the correct authorization of the end user via user identification character and password;

c) the version number of the software and contents (to determine if the version is potentially out of date);

d) the type of the software and contents to be used with respect to a *preset profile of the end user* (e.g., restriction with respect to specific contents for accounts of under age persons, etc .); and

e) the *creditworthiness and account balance of the end user.* [Specification at page 9 lines 5-30; emphasis added.]

Because Krishnan's system requires an Electronic License Certificate ("ELC") to be installed on DCS Client 301, Krishnan teaches away from the system defined by claim 5. Therefore, Krishnan does not disclose or suggest all the limitations of claim 5. Therefore, claim 5 is not anticipated by Krishnan. Therefore, the rejection of claim 5 under 35 USC 102(e) is improper and should be reversed.

C. The Rejections Under 35 USC 102(e) of Dependent Claims 6-8

1. The Citations Relied Upon By the Examiner

The citations to Krishnan relied upon by the examiner in rejecting claims 6-8 are included

in the citations to Krishnan used in rejecting claim 5 above.

2. **Claims 6-8 - Dependency On Allowable Claims**

In reply, the applicant respectfully traverses these rejections because they are not supported by either substantial evidence or proper legal conclusions. The rejected claims depend directly from claim 5. Therefore, the rejected claims are patentably distinguishable over Krishnan for at least the reasons given above for claim 5. Therefore, the rejections of claims 6-8 are improper and should be reversed.

D. **The Rejection Under 35 USC 102(e) of Dependent Claim 9**

1. **The Citations Relied Upon By the Examiner**

The citations to Krishnan relied upon by the examiner in rejecting claim 9 are included in the citations to Krishnan used in rejecting claim 1 above.

2. **Claim 9 - Dependency On An Allowable Claim**

In reply, the applicant respectfully traverses this rejection because it is not supported by either substantial evidence or proper legal conclusions. The rejected claim depends directly from claim 5. Therefore, the rejected claim is patentably distinguishable over Krishnan for at least the reasons given above for claim 5.

3. **Claim 9 - Krishnan Does Not Teach or Suggest "...performing a usage charging of said software product on user accounts and provider accounts..."**

Claim 9 recites "...performing a usage charging of said software product on user accounts and provider accounts...." The citation to Ahmad relied upon by the examiner in rejecting claim 9 does not disclose or suggest "....performing a usage charging of said software product on user accounts and provider accounts...." Therefore, claim 9 is patentably distinguishable over Krishnan and Ahmed. Therefore, the rejection of claim 9 is improper and should be reversed.

E. **The Rejection Under 35 USC 102(e) of Dependent Claim 10**

1. **The Citations Relied Upon By the Examiner**

The citations to Krishnan relied upon by the examiner in rejecting claim 10 are included in the citations to Krishnan used in rejecting claim 1 above.

2. **Claim 10 - Dependency On An Allowable Claim**

In reply, the applicant respectfully traverses this rejection because it is not supported by either substantial evidence or proper legal conclusions. The rejected claim depends directly from claim 5. Therefore, the rejected claim is patentably distinguishable over Krishnan for at least the reasons given above for claim 5.

3. **Claim 10 - Krishnan Does Not Teach or Suggest a "...usage processing module keeps statistics about usage contacts that have taken place and about results of a processing of said usage contacts..."**

Claim 10 recites a "...usage processing module keeps statistics about usage contacts that have taken place and about results of a processing of said usage contacts...." The citation to Ahmad relied upon by the examiner in rejecting claim 10 does not disclose or suggest a "...usage processing module keeps statistics about usage contacts that have taken place and about results of a processing of said usage contacts...." Therefore, claim 10 is patentably distinguishable over Krishnan and Ahmed. Therefore, the rejection of claim 10 is improper and should be reversed.

F. **The Rejection Under 102(e) of Claim 11**

Claim 11 defines the same imitations as claim 5, which, as discussed above, are not disclosed or suggested by Krishnan. Therefore, the applicant respectfully submits that claim 11 patentably defines over Krishnan for at least the reasons given above for claim 5. Therefore, the applicant respectfully submits that the rejection of claim 11 under 35 USC 102(e) over Krishnan is improper and should be reversed.

G. **The Rejections Under 35 USC 102(e) of Dependent Claims 12 and 13**

1. **The Citations Relied Upon By the Examiner**

The citations to Krishnan relied upon by the examiner in rejecting claims 12 and 13 are included in the citations to Krishnan used in rejecting claim 1 above.

2. **Claims 12 and 13 - Dependency On An Allowable Claim**

In reply, the applicant respectfully traverses this rejection because it is not supported by either substantial evidence or proper legal conclusions. The rejected claims depend directly or

indirectly from claim 11. Therefore, the rejected claims are patentably distinguishable over Krishnan for at least the reasons given above for claims 1, 5, 11, and 14.

3. **Claims 12 and 13 - Krishnan Does Not Teach or Suggest "...dynamically determined user data..."**

Claims 12 and 13 recite "...dynamically determined user data...." The citation to Ahmad relied upon by the examiner in rejecting claims 12 and 13 does not disclose or suggest a "...dynamically determined user data...." Therefore, claims 12 and 13 are patentably distinguishable over Krishnan and Ahmed. Therefore, the rejections of claims 12 and 13 are improper and should be reversed.

H. The Rejections Under 102(e) of Independent Claim 14

1. The Examiner's Argument

The examiner's arguments in rejecting claim 14 are substantially the same as for claim 5 above.

2. The Citations to Krishnan Relied Upon By the Examiner

The citations to Krishnan relied upon by the examiner in rejecting claims 14 are included in the citations to Krishnan used in rejecting claim 5 above.

3. The Applicant's Traversal of the Rejections

In reply, the applicant respectfully traverses these rejections for the same reasons noted above for claim 5 because they are not supported by either substantial evidence or proper legal conclusions. Claim 5 recites a "usage processing server...operated by a network provider." Claim 14 recites "a usage processing server...operated by a network provider." For the reasons just stated, Krishnan does not disclose or suggest "...a usage processing server...operated by a network provider...". Therefore, claim 14 is patentably distinguishable over Krishnan for at least the reasons given above for claim 5. Therefore, the rejections of claim 14 is improper and should be reversed.

I. The Rejections of Claims 1, 3, 4, and 15 Under 35 USC 103(a) as Being Unpatentable Over Krishnan et al. (US Patent No. 6,073,124) in view of

Ahmad (US Patent No. 5,925,127)

The examiner rejects claims 1, 3, 4, and 15 under 35 U.S.C. 103(a) as being unpatentable over Krishnan et al. (U.S. Patent No. 6,073,124) in view of Ahmad (U.S. Patent No. 5,925,127), stating that:

> As per claims 1 and 15, Krishman et al teaches a method of using software products that are offered via a network comprising inquiring about a software product from an offer server by a user via a terminal device downloading the software product from the offer server via the network onto the terminal device in response to the inquiry of the user activating a software component of the software product starting a communication by way of the software component with a usage processing server regarding a usage of the software product in response to a call of the software product in the terminal device of the usèr, providing, by the software component in a framework of the communication, data to the usage processing server (*see figs 2, 3, summary of the invention and column 6 lines 44-7 lines 43, 8 lines 33-12 line 59*). Krishman et al fails to teach an inventive concept of checking the data, by the usage processing server, and then making a determination selected from the group consisting of: whether usage of the software product is approved with respect to the inquiring user, and whether charging operations are carried out on user accounts and provider of software product accounts. However, Ahamad teach an inventive concept of checking the data, by the usage processing server, and then making a determination selected from the group consisting of whether usage of the software product is approved with respect to the inquiring user, and whether charging operations are carried out on user accounts and provider of software product accounts (*see fig 3, column 9 line! 5-12 line 10*). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Krishman et al's inventive concept to include Ahamad's inventive concept and checking the data, by the usage processing server, and then making a determination selected from the group consisting of whether usage of the software product is approved with respect to

the inquiring user, and whether charging operations are carried out on user accounts and provider of: software product accounts because this would have facilitate [sic] software application provider to monitor the usage of their software application usage thereby increase [sic] the revenue of the provider. [Office Action mailed October 12, 2004 page 6 line 18 through page 7 line 20; interpolation provided.]

1. **The Rejections Under 35 USC 103(a) of Claim 1**

a. **The Recitation of Claim 1**

1. A method for using software products that are offered via a network, comprising:

inquiring about a software product from an offer server by a user via a terminal device;

downloading said software product from said offer server via said network onto said terminal device in response to said inquiring by said user;

activating a software component of said software product;

starting a communication by way of said software component with a usage processing server regarding a usage of said software product in response to a call of said software product in said terminal device of said user, wherein said usage processing server is operated by a network provider;

providing, by said software component in a framework of said communication, data to said usage processing server; and

checking said data, by said usage processing server, and then making a determination selected from a group consisting of: whether usage of said software product is approved with respect to said inquiring user, and whether charging operations are carried out on user accounts and provider of software product accounts.

b. **The Citations Relied Upon By the Examiner**

In rejecting claims 1, 3, 4, and 15, the examiner relies on the same passages from

Krishnan cited in the rejections of claims 5-14. In rejecting claims 1, 3, 4, and 15, the examiner in the office action mailed March 24, 2004, at pages 6-7 item 17, also relies on the following passage from Ahmad at column 9 line 15 to column 12 line 10, which states that:

> FIG. 3 is a simplified block diagram illustrating the downloading of software program modules embodying an exemplary embodiment of the present invention from a remote server to a user's computer 20 via the Internet 60. Generally, as illustrated in FIG. 3, program modules available for rental are registered with a central registration site, such as a Software Registry 95. In the exemplary embodiment illustrated in FIG. 3, the Software Registry 95 is maintained on the program module rental server 88a. It should be understood that the Software Registry 95 may be maintained at a different location or remote server separate from the program module rental server 88a. It should also be understood that a variety of software program module owners or developers may register their program modules on the Software Registry 95 for rental to prospective users by the rental service provider. It should further be understood that any number of rental service providers may be authorized to rent a particular software program module which is registered with the Software Registry 95. Preferably, each rental service provider will rent that particular program module from their respective Internet servers.
>
> After the rental form is completed by the user, the rental service provider issues from the rental server 80a an instance of a Check-in/Check-out (CICO) module 120 corresponding to the particular program module 100 requested by the user. As is discussed in detail below, the CICO module 120 contains required licensing information for the program module requested by the user.
>
> The program module 100 and the corresponding CICO module 120 are downloaded from the server 80a (in no particular order) to the user's computer 20 over the Internet 60, illustrated in FIG. 3, in a manner well known to those skilled

in the art. Both modules are typically stored on the user's hard disk drive, or some other form of non-volatile memory storage device. As is well known to those skilled in the art, one or both of the modules (program module 100 and CICO module 120) can be compressed to expedite the downloading process. That is, the program module 100 may, if desired, be appended to the CICO module 120 to form one module. That one module may be downloaded to the user's computer 20, as described above.

Once the program module 100 and the CICO module 120 are downloaded onto the user's computer 20, the CICO module 120 provides the licensing information to a Software Monitor module 140 that is resident on the user's computer 20. In the case of a single module combining the CICO module 120 and the program module 100, the CICO module 120 will run first to provide the required licensing information to the Software Monitor module 140. As is discussed in detail below, the Software Monitor module is a software application that monitors and ensures that use of the rented program module 100 by the user is in accordance with the licensing information provided by the CICO module 120. The operation and interaction of the processes and software program modules embodying the present invention discussed above will now be discussed in detail.

Referring now to FIGS. 2 and 3, as discussed above, before a particular program module 100 may be rented, that program module 100 must be registered on a Software Registry 95, which is a central registration site which may be maintained on the rental service provider's server 88a or separately from the rental service provider's server 88a. In response to registration on the Software Registry, the Software Registry assigns the program module 100 a unique identification number (APPID). For example, Microsoft "Word," version 8.0, would receive an APPID. If the program module 100 already has an assigned APPID, the Software Registry 95 will register this pre-assigned APPID, which is typically provided by the

manufacturer of the program module 100. For example, the APPID can be a "Global Unique Identifier code" (GUID) assigned to selected program module titles by software manufacturers.

The CICO module 120 is a software program module responsible for providing licensing information for the rented program module 100 to the Software Monitor module 140 (discussed below) resident on the user's computer 20. The licensing information contained by the CICO module 120 includes the APPID and the licensed period of time over which the program module 100 may by used. The CICO module 120 is a tool that will encode this information on the user's computer 20 so that the Software Monitor module 140 can be made aware of the user's permission to use the program module 100, as well as the time period over which use of the program module 100 is allowed. It should be understood that a CICO module 120 is downloaded each time a program module is rented or renewed.

The CICO module 120 must be run on the user's computer 20 prior to running the rented program module 100 on the user's computer 20. In the preferred embodiment, the CICO module 120 is downloaded from the rental server 88a via the Internet, as described above. The CICO module 120 is preferably implemented as a dynamic-link library module (DLL) or as an Active X/OLE module (OCX). These types of modules are well known to those skilled in the art as modules that serve a specific function or set of functions which may be launched only when needed by a program that calls them. Preferably, the CICO module 120 is launched upon being downloaded to the user's computer 20. The mechanism for downloading and launching the CICO module 120 from the Internet is well known to those skilled in the art.

Because the CICO module 120 is a software application itself, it must be made

secure from unauthorized copying or tampering before it can assist in securing the rented program module. Each CICO module has a CICO module identification number (CID). The CID preferably has two parts separated by a "-". As is discussed in detail below, the first part of the CID is a unique identification number generated and encode into the CICO module by the Software Monitor module 140, and the second part is the identification number unique to the user's computer 20. The Software Monitor module 140 verifies the CICO module 120 has not been used before and then issues a randomly generated unique CID to the CICO module 120. After the CICO module 120 provides the Software Monitor module 140 with the licensing information for the rented program module 100, the CICO module 120 is deleted by the Software Monitor module 140 to prevent any unauthorized copying of the CICO module 120.

Upon downloading the program module 100 and the CICO module 120 onto the user's computer 20, the program module 100 will load the Software Monitor module 140 (SM) for operation. As should be understood from the foregoing discussion, the SM 140 is a software program module or module that verifies the user's license to use the rented program module and tracks use of the rented program module by the user. Referring to FIG. 3, the SM 140 may be downloaded from the rental server 80a to the user's computer 20 at the time the program module 100 and the CICO module 120 are downloaded. Alternatively, the SM 140 may be resident on the user's computer 20 as part of software provided to the user on the computer's hard disk drive.

The SM 140 must run constantly on the user's computer 20 during use of the rented program module 100 to prevent unauthorized use of the rented program module 100. As with the CICO module 120, the SM 140 may be implemented as either a system DLL or an ActiveX control module. Once the CICO module 120 has been downloaded and secured by the SM 140, as discussed above, the CICO

module 120 transfers to the SM 140 the license information for the rented program module. The data is transferred as bytes to the SM 140 in a manner well known to those skilled in the art. The SM 140 is responsible for interpreting and using the information. The task of the CICO module 120 is completed as soon as the information is transferred.

The SM 140 tracks the time of use of the program module 100 without the use of the computer's system clock because the computer's system clock may be easily changed by the user. The SM 140 utilizes an internal timer to track the actual elapsed time of use of the program module 100. The standard approach to calculating the time of use is to subtract the start time, i.e., the time the program module 100 is launched from the end time, i.e., the time the program module 100 is exited.

To further prevent the user from manipulating the system, the SM 140 may hook into the system clock of the computer 20 via the operating system, which offers system time and system date, to be notified each time the system clock is changed. Consequently, all changes to the system clock will be recorded and accounted for by the SM 140.

Alternatively, the SM 140 may track the number of uses of the program module 100 if the program module is rented for a specified licensed number of uses. The SM 140 may track the number of uses of the program module 100 by setting an internal counter, similar to the above-described internal timer, when the program module 100 is first used. Upon each subsequent licensed use, the counter will add one count. The SM 140 will compare the total count to the licensed number of uses each time the user attempts to launch the program module 100. After the licensed number of uses is expended the SM 140 will prevent subsequent operation of the program module 100.

For subsequent use of the program module 100, the SM 140 can remember that it deleted the CICO module 120 during the first use of the program module 100, and the SM 140 will not check for the CICO module 120 on the second (and future uses) of the program module 100 while time remains for use of the program module 100. For subsequent rental of the program module 100, there is no need to download the program module 100 again. However, there is a need to download the CICO module 120 again from the rental service provider's server each time the program module 100 is subsequently rented.

Unauthorized copying of the program module 100 is prevented by rendering the program module useless without the simultaneous operation of the Software Monitor 140. Because the program module 100 will not run without the simultaneous running of the SM 140, any unauthorized copy of the program module 100 launched on a different computer will be rendered useless because the SM 140 will recognize that the computer identifier for the different computer does not match the computer identifier stored as a part of the unique CID, described above. Accordingly, the SM 140 will not allow the unauthorized copy of the program module 100 to run. [Ahmad at column 9 line 15 to column 12 line 10.]

c. **Ahmad Does Not Teach or Suggest "...a usage processing server...operated by a network provider..." As Recited By Claim 1**

In reply, the applicant respectfully submits that Ahmad does not teach or suggest "...a usage processing server...operated by a network provider..." as recited by claim 1.

i. **Ahmad's "Web Server" Is Not the Claimed "Network Provider" As Recited By Claim 1**

Ahmad discloses at column 8 lines 1-38 that:

...The Internet 60 includes a plurality of backbone networks 65a through 65n. These backbone networks form an international grid of high-speed, high-capacity data communication lines interconnecting a number of massive computers that serve as large-scale processing points or nodes. The backbone networks 65 are interconnected with each other through a plurality of network access points 70a through 70n. These network access points are interfaces through which information is communicated from one backbone network to another....

The Internet 60 includes a plurality of *Internet sites* 75a through 75n. These Internet sites are generally *operated by corporations, universities, and governmental organizations*. Each Internet site may include one or more repositories of information and resources that may be accessed over the Internet. Each Internet site, as represented by the Internet site 75a, may include a plurality of *web servers* 80a through 80n. Each of these web servers may provide "home pages" to be visited, files to be read or downloaded, *applications to be shared*, and the like. [Ahmad at column 8 lines 1-38; emphasis added.]

The Internet 60 also includes a plurality of *points of presence* 85a through 85n that are *operated by local access providers*. These local access providers are in the business of *providing Internet access to end user stations*. In the preferred embodiment of the present invention, the personal computer 20, shown in FIG. 1, is an end-user station. As shown in FIG. 2, the point of presence 85a provides Internet access to the personal computer 20 (end user station) and other end user

stations 88a through 88n, the point of presence 85b provides Internet access to end user stations 88a' through 88n', etc. All together, the points of presence 85 can provide Internet access to numerous end-user stations 88. Each point of presence 85, and each end user 88, may, but need not, provide home pages for access by others on the Internet 60. [Ahmad at column 8 lines 1-38; emphasis added.]

In fact, Ahmad's Internet sites and web servers are designed to provide "repositories of information" and to be "operated by corporations, universities, and governmental organizations." Thus, clearly Ahmad's "Internet sites" and "web servers" are not designed to provide network connectivity for the end user.

ii. **Ahmad Discloses "Applications to be Shared" and a "Rental Service Provider" Residing on His "Web Server," Not "...a usage processing server...operated by a network provider..." As Recited By Claim 1**

It is clear that the only components in Ahmad's system designed to provide shared applications, that is, applications that may be downloaded from the Internet, are Ahmad's Internet sites and web servers:

Each Internet site, as represented by the Internet site 75a, may include a plurality of *web servers* 80a through 80n. Each of these web servers may provide "home pages" to be visited, files to be read or downloaded, *applications to be shared*, and the like. [Ahmad at column 8 lines 1-38; emphasis added.]

It is also clear that the only components in Ahmad's system designed to provide a "rental service" are Ahmad's Internet sites and web servers:

Referring now to FIG. 2, a user desiring to rent a particular program module, logs onto the Internet, as discussed above, and accesses the *Internet site 75a of the software rental service provider.* The user then locates the *rental server 80a at the Internet site 75a.* The user completes a rental form provided on the server 80a and requests use of a particular program for a specified period of time.

> It should be understood that the form can also require payment information, such as a credit card number or an account number if the user has an established account with the rental service provider. [Ahmad at column 8 lines 54-64; emphasis added.]

Therefore, the only component of Ahmad's system that could possibly have been recognized by one of ordinary skill in the art as the claimed "usage processing server" would have been Ahmad's "web servers" operated by Ahmad's "Internet sites." No other component in Ahmad's disclosed system has the capability to function as the claimed "usage processing server." Most importantly, Ahmad does *not* disclose that his "points of presence 85a through 85n" provide "applications to be shared" or a "rental service provider."

iii. **Only Ahmad's "Points of Presence" May Function As the Claimed "Network Provider," But Does Not Disclose That His "Points of Presence" Provide "Applications to be Shared" or a "Rental Service Provider"**

In Ahmad's system, the only component which would have been recognized by one of ordinary skill in the art as being the claimed "network provider" would have been Ahmad's points of presence. However, Ahmad states that:

> The Internet 60 also includes a plurality of *points of presence* 85a through 85n that are *operated by local access providers*. These local access providers are in the business of *providing Internet access to end user stations*. [Ahmad at column 8 lines 24-28; emphasis added.]

Thus, Ahmad clearly distinguishes the functionality of his "points of presence 85a through 85n" from his "Internet sites 75a through 75n" and his "web servers 80a through 80n" because Ahmad discloses that only Ahmad's "point of presence" provide Internet access to "end user stations." In contrast, as noted above, Ahmad's Internet sites and web servers are designed to provide "repositories of information" and to be "operated by corporations, universities, and governmental organizations."

iv. **Ahmad Does Not Disclose That His "Points of Presence" Provide "Applications to be Shared" or a "Rental Service Provider"**

As noted above, Ahmad only discloses that web servers 80a-80n provide "applications to be shared" and a "rental service provider." Ahmad does *not* disclose that his "points of presence 85a through 85n" provide either "applications to be shared" or a "rental service provider."

Therefore, there is no teaching in Ahmad that suggests "...a usage processing server...operated by a network provider...," recited by claim 1 and defined in this application. Therefore, Ahmad in combination with Krishnan does not teach or suggest the subject matter of claim 1. Therefore, the rejection of claim 1 under 35 USC 103(a) over Krishnan in view of Ahmad is improper and should be reversed.

d. **No Motivation to Combine References**

The applicant respectfully submits that one of ordinary skill in the art would *not* have been motivated to combine the teachings of Ahmad with the teachings of Krishnan. Because there is no teaching or suggestion to combine the teachings of Ahmad with the teachings of Krishnan, the examiner has not made a proper *prima facie* rejection. Therefore, the rejection of claim 1 under 35 USC 103(a) over Krishnan in view of Ahmad is improper and should be reversed.

2. **The Rejection Under 103(a) of Dependent Claim 3**

a. **The Citations Relied Upon By the Examiner**

The citations to Krishnan relied upon by the examiner in rejecting claim 3 are included in the citations to Krishnan used in rejecting claim 1 above.

b. **Claim 3 - Dependency On An Allowable Claim**

In reply, the applicant respectfully traverses this rejection because it is not supported by either substantial evidence or proper legal conclusions. The rejected claim depends directly from claim 1. Therefore, the rejected claim is patentably distinguishable over Krishnan for at least the reasons given above for claims 1, 5, 11, and 14. Therefore, the rejection of claim 3 is improper and should be reversed.

c. **Claim 3 - Krishnan Does Not Teach or Suggest "...operating said offer server by a network provider..."**

Claim 3 recites "...operating said offer server by a network provider...." The citation to Ahmad relied upon by the examiner in rejecting claim 3 does not disclose or suggest "...operating said offer server by a network provider...." Therefore, claim 3 is patentably distinguishable over Krishnan and Ahmed. Therefore, the rejection of claim 3 is improper and should be reversed.

3. **The Rejection Under 103(a) of Dependent Claim 4**

a. **The Citations Relied Upon By the Examiner**

The citations to Krishnan relied upon by the examiner in rejecting claim 4 are included in the citations to Krishnan used in rejecting claim 1 above.

b. **Claim 4 - Dependency On An Allowable Claim**

In reply, the applicant respectfully traverses this rejection because it is not supported by either substantial evidence or proper legal conclusions. The rejected claim depends directly from claim 1. Therefore, the rejected claim is patentably distinguishable over Krishnan for at least the reasons given above for claims 1, 5, 11, and 14. Therefore, the rejection of claim 4 is improper and should be reversed.

c. **Claim 4 - Krishnan Does Not Teach or Suggest "...a server selected from the group consisting of said offer server and said usage processing server..."**

Claim 4 recites "...a server selected from the group consisting of said offer server and said usage processing server...." The citation to Ahmad relied upon by the examiner in rejecting claim 4 does not disclose or suggest "...a server selected from the group consisting of said offer server and said usage processing server...." Therefore, claim 4 is patentably distinguishable over Krishnan and Ahmed. Therefore, the rejection of claim 4 is improper and should be reversed.

4. **The Rejection Under 103(a) of Independent Claim 15**

a. **The Citations Relied Upon By the Examiner**

The citations to Krishnan and Ahmad relied upon by the examiner in rejecting claim 15 are included in the citations to Krishnan and Ahmad used in rejecting claim 1 above.

b. **The Applicant's Traversal of the Rejection: No Motivation to Combine References**

In reply, the applicant respectfully traverses this rejection because it is not supported by either substantial evidence or proper legal conclusions. One of ordinary skill in the art at the time of the invention would not have been motivated to combine the teachings of Krishnan with the teachings of Ahmad for the reasons given above for claim 1. Therefore, the examiner has not made an proper *prima facie* rejection. Therefore, the rejection of claim 15 is improper and should be reversed.

Respectfully Submitted,

4/11/2005 Robert G. Crockett

Date Robert G. Crockett

Registration No. 42,448

VIII. **37 CFR 41.37(c)(1)(viii) Claims Appendix**

Claims On Appeal

1. A method for using software products that are offered via a network, comprising:

inquiring about a software product from an offer server by a user via a terminal device;

downloading said software product from said offer server via said network onto said terminal device in response to said inquiring by said user;

activating a software component of said software product;

starting a communication by way of said software component with a usage processing server regarding a usage of said software product in response to a call of said software product in said terminal device of said user, wherein said usage processing server is operated by a network provider;

providing, by said software component in a framework of said communication, data to said usage processing server; and

checking said data, by said usage processing server, and then making a determination selected from a group consisting of: whether usage of said software product is approved with respect to said inquiring user, and whether charging operations are carried out on user accounts and provider of software product accounts.

2. (Canceled)

3. The method of claim, further comprising operating said offer server by a network provider.

4. The method of claim 1, further comprising using a web server for a server selected from the group consisting of said offer server and said usage processing server.

5. A usage processing server comprising:

a usage processing module for processing a software product downloaded from a network;

wherein said usage processing server is operated by a network provider and wherein said usage processing server is contacted by said software product after said software product has been downloaded into a terminal device of a user and has been activated; and

wherein usage processing data required to perform usage processing are delivered to said usage processing server.

6. A usage processing server according to claim 5, further comprising:

a data store in which a software product identification of said software product and type of usage processing data that prescribe a type of usage processing of said software product are stored by said usage processing module, and

wherein said usage processing module registers said software product.

7. A usage processing server according to claim 5, wherein:

said usage processing data required comprises a software product identification of said software product and a user identification.

8. A usage processing server according to claim 5, wherein:

said usage processing comprising performing an access control.

9. A usage processing server according to claim 5, wherein:

said usage processing comprises performing a usage charging of said software product on user accounts and provider accounts.

10. A usage processing server according to claim 5, wherein:

said usage processing module keeps statistics about usage contacts that have taken place and about results of a processing of said usage contacts.

11. A software product, comprising:

a software component that is activated when called by said software product and that subsequently starts communicating with a usage process server and delivers usage processing data required for performing usage processing to said usage processing server in the framework of said communication, wherein said usage processing server is operated by a network provider;

wherein said software product can be downloaded into a terminal device by a user via a network in response to an inquiry from said user.

12. A software product according to claim 11, wherein said usage processing data comprises:

software product provider data;

software product identification; and

wherein said usage processing data is dynamically determined user data.

13. A software product according to claim 12, wherein said software component interacts with said user to produce said dynamically determined user data.

14. A method for the generation of a software product that is offered via a network, comprising:

installing a software component in source code of said software product of a software manufacturer by using a software development kit provided by a usage processing provider;

activating said software component when called by said software product;

starting a communication by said software component with a usage processing server after said activating said software component, wherein said usage processing server is operated by a network provider;

sending, by said software component, usage processing data that are required for performing usage processing to said usage processing server in the framework of said communication.

15. A method for using software products that are offered via a network, comprising:

inquiring about a software product from an offer server by a user via a terminal device;

downloading said software product from said offer server via said network onto said terminal device in response to said inquiring by said user;

activating a software component of said software product;

starting a communication by way of said software component with a usage processing server regarding a usage of said software product in response to a call of said software product in said terminal device of said user;

providing, by said software component in a framework of said communication, data to said usage processing server; and

checking said data, by said usage processing server, and then making a determination selected from a group consisting of: whether usage of said software product is approved with respect to said inquiring user, and whether charging operations are carried out on user accounts and provider of software product accounts.

IX. **37 CFR 41.37(c)(1)(ix) Evidence Appendix**

This section is not applicable in this appeal.

X. **37 CFR 41.37(c)(1)(x) Related Proceedings Appendix**

This section is not applicable in this appeal.

RGC
Printed: April 11, 2005 (3:20pm)
Y:\Clients\Siemens\SIEM0023UUSCP\Drafts\AppealBrief_050411.wpd